

Amendments to the Specification

Please **replace** the paragraph beginning at page 1, line 5 with the following **rewritten** paragraph:

~~-- This application claims the benefit of U.S. Provisional Application No. 60/454,551, filed March 14, 2003, and incorporated herein by reference.~~

This application claims the benefit, under 35 U.S.C. § 365 of International Application PCT/US04/07806, filed March 12, 2004, which was published in accordance with PCT Article 21(2) on September 30, 2004 in English and which claims the benefit of United States provisional patent application No. 60/454,551, filed March 14, 2003. --

Please **replace** the paragraph beginning at page 1, line 9 with the following **rewritten** paragraph:

-- The invention provides an apparatus and a method for in which a client terminal is automatically configured for access to a communications network, and in particular, a WLAN system automatically configures an IEEE 802.1x client on the wireless user device through the client web browser and an ActiveX control or a functionally equivalent plug-in. The IEEE 802.1x client configured in this manner is then able access with the WLAN system using the appropriate authentication parameters.--

Please **replace** the paragraph beginning at page 3, line 1 with the following **rewritten** paragraph:

-- The invention herein provides a method for automatically configuring an IEEE 802.1x client terminal to provide ~~limited~~ secure access in a ~~WLAN~~ wireless local area network environment comprising the steps of the ~~WLAN~~ filtering traffic associated with ~~the limited access and thereby~~ an HTTP request from the client terminal for access to the wireless network redirecting ~~the client terminal~~ the HTTP request to a designated web server, ~~whereby the web server responds to the client terminal~~ and issuing a request from the designated web server to the client terminal

~~for by requesting~~ information required to establish an authorized communication.

Thereafter, the client terminal provides the web server information required to establish an authorized communication. In the course of the communication the web server indicates to the client terminal information corresponding to such parameters as transmission rates, user account requirements, authentication method selection information, new account creation procedures, user terms and conditions which are all typically required to establish an authorized communication. The client terminal user responds accordingly with web server access rate information, web server user account creation information, user access authentication method selection information, and user acceptance of the offered service required to establish an authorized communication.--

Please **replace** the paragraph beginning at page 3, line 19 with the following **rewritten** paragraph:

-- The present invention also includes one or more apparatus that cooperate in providing a secure communications session between a client terminal 140_n and a WLAN. The client terminal requests access to the WLAN through an access means. The WLAN processes the request sending it to a packet filter that redirects the client to a designated web server. The web server responds by providing provider list web pages, which are processed by means where the user inputs its selection and sends the client terminal access information. The web server responds by sending an ActiveX Control to configure the client terminal utilizing a means for activating, in response to the information received from the client terminal, a software module that reconfigures the client terminal and establish an authorized communication. Thereafter the client access means permits authenticated access to pass through the WLAN. The WLAN provides a means for authenticating the reconfigured client terminal and allows access to the WLAN in response to the authentication using appropriate parameters associated with a configuration arrangement selected by a user.--

Please **replace** the paragraph beginning at page 6, line 12 with the following **rewritten** paragraph:

-- The access point includes an IEEE 802.1X engine 325, which is a module that implements the IEEE 802.1X protocol with the determining means necessary to carry out the steps of the present invention. The WLAN 115 system must maintain proper state information for the system to function properly. Such state information will be provided by the access point 130_n IEEE 802.1x engine, which is used by, among other things, the packet filtering function 330 and the HTTP server 120. With reference to FIG. 2, a further embodiment of the present invention is the utilization of the access point 130_n to create several operational states. Following a Response-Identity EAP packet 220 a state 1x_progress 340 indicates that the mobile terminal 140_n is an IEEE 802.1x client and the IEEE 802.1x authentication process is ongoing. Such means to select from one or more available security protocols is well known by those skilled in the art of programming and engineering in a WLAN environment. The IEEE 802.1X engine 325 is therefore responsible for client detection and providing the client capability information to other modules of the system. In addition, it also implements RADIUS client functionality to convert EAP messages to RADIUS messages, forwarding such messages in the form of a radius access request 230 and responding to radius access reject messages 240. The packet filter module 330 is responsible for filtering packets based on the criteria set by other modules.--

Please **replace** the paragraph beginning at page 6, line 29 through page 7, line 7 with the following **rewritten** paragraph:

-- In the event, a EAP-Response-Identity packet 220 results in a state 1x_failure 350 because, as by way of example, the client is not properly configured, the client would be redirected to the local HTTP server 120 to attempt a reconfiguration of the client. More particularly, FIG. 2 illustrates an embodiment of the method of the present invention wherein the access point 130_n detects that the mobile terminal 140_n is not an authenticated IEEE 802.1x client, and a redirected client 335 moves the process to thereby configure through an IP packet filter module 330 and move the process to the HTTP server 120 via a web request redirect 345.

Alternatively, mobile terminal 140_n may send a direct web access request 355, which is redirected by the packet filter module 330 to the HTTP server 120. When the HTTP server 120 receives a web redirect request 345 it responds by presenting the mobile terminal 140_n with information 360, such as a provider list web page, specifically related to the browser based authentication. --

Please **replace** the paragraph beginning at page 7, line 13 with the following **rewritten** paragraph:

-- The invention herein provides a method for automatically configuring a IEEE 802.1x client terminal to provide limited secure access in a WLAN wireless local area network 115 comprising the steps of an access point 130_n filtering traffic 330 associated with ~~the limited access and thereby~~ an HTTP request from the client terminal for access to the wireless network redirecting ~~via a web request redirect 345~~ the HTTP to a client terminal 140_n to the designated HTTP web server 120, whereby ~~the web server responds to the client terminal 140_n by sending~~ and issuing a request from the designated web server to the client terminal 140_n for information 360 required to establish an authorized communication. Thereafter the client terminal 140_n provides the web server information 365 such as the provider selected, to establish an authorized communication. In the course of the communication the web server 120 indicates to the client terminal 140_n information corresponding to such parameters as transmission rates, user account creation information, authentication method selection information, new account creation procedures, access user terms and conditions of acceptance, all typically required to establish an authorized communication. The client terminal 140_n user responds 365, accordingly communicating web server 120 access rate information, web server user account creation information, user access authentication method selection information, and user access terms and conditions of acceptance information required to establish an authorized communication. The HTTP server 120 invokes 370 a plug-in such as an ActiveX control plug to assist the terminal 140_n in reconfiguring 375 the terminal 140_n.--

Please **replace** the paragraph beginning at page 7, line 30 with the following **rewritten** paragraph0:

-- In referring to FIG. 3, the present invention also includes an apparatus for providing a secure communications session between a client terminal 140_n and a WLAN 115. The client terminal 140_n requests through means 445 access to the WLAN 115 through the access point 130_n receiver ~~405~~ 415, which processes the request through means 418 and sends the request to a packet filter 420 that redirects the client to a designated web server via transmit means 424. The web server responds to the client terminal 140_n by providing provider list web pages, which are processed by means 448 where the user inputs its selection through a means 448 and sends the client terminal 140_n access information through transmit means 470. The web server responds by sending an ActiveX Control to configure the client terminal 140_n utilizing a means 465 for activating, in response to the information received from the client terminal, a software module that reconfigures the client terminal and establish an authorized communication. Thereafter the client access means 480 permits authenticated access to pass through the WLAN 115. The access point 130_n provides a means for authenticating the reconfigured client terminal and allows access to the WLAN in response to the authentication using appropriate parameters associated with a configuration arrangement selected by a user.--